Role-Based Security for PCI

Your system gathers and stores data that is essential to the company's success. One of your first priorities should be to protect that data by making sure that only authorized staff can access it.

Objectives

- Activating RBS
- High-Security Passwords
- Setting Up Alerts

Activating RBS

Let's start by creating user records in the system. From the Home page, Select *System Management,* then *Security Maintenance,* and click *Role-Based Security Maintenance.*

Click the *Miscellaneous* button and then choose *Add/Delete/Change User*. Click number 1*, Add a User.* Fill out as much information as you can. To add another user, follow the same steps. You can have as many users as possible but there should be at least two roles with six security bits.

In the *Launch* bar, enter *OPT*. Select *Option ID* and enter *550. Option ID 550* opens the Role-based security screen. Make sure this is activated. Roles must be created after *RBS* has been activated to assign users to roles. This is similar to the idea of copying one user security to another in terminal-based security.

To create roles, enter *RBS* in the *Launch* bar. Select *MISC* and choose *Maintain Roles.*
In the *Maintain Role* page, select the *MISC* option and then choose *Create Role from Standard Role.*

From the *Role* drop-down menu, select a standard role such as *System* or *ADMIN,* with the security bits set to yes. We recommend one "*Admin*" role with the six security bits that trigger high-security passwords, and as many other roles as desired, none of which contain any of the six security bits listed. 14, 91, 506, 689, 691, 757.

Enter the same value in the *Save As* field. Click *Ok.*

In the *Role-Base Security* page, select a user and press enter. There should be at least two *users* assigned to this role that will have high security passwords.

This is to prevent getting locked out of the system if the password expires, or gets too many failed attempts for one High Security Password User

If the user is set to terminal-based security, then click the hyperlink *Type: Terminal Based Security.* In the *Enable Role-Based Security* pop-up, select *OK*. Now, select *Role-Based Security* and click *OK.*

The user login will display available roles. To select the roles, click in the box for each store so that *Yes* displays in each store field. Finally, click *Change* to save.

High-Security Passwords

Now that you have created users and assigned at least two users to the *admin* role.
Let's Follow these steps to check all other roles for these six security bits and to set these bits to NO for all roles except for the "*admin*" role that has these bits set to Y. The six security bits are *Option ID 14, 91, 506, 689, 691, and 757.*

To check if the option IDs are enabled, enter *MSE* in the *Launch* bar. Select *MISC* and then choose *Review Security Bit Usage for Terminals.*

Enter the security bit, terminal, and store. A list of users with the security bit set to *YES* will be displayed.
Repeat the process for the remaining security bits.

You should only add the user that need these six security bits to the "admin" role that contains these bits.

All users in this role should convert to a high-security password before flipping the PCI flag.
If the PCI flag is flipped before converting to a high-security password, these users in this role will be locked out until they convert to a high-security password.

There should be at least two users in this role, but it could be as many as the owner desires. To change a password, enter *RBS* in the *Launch* bar.

Select *MISC* and then choose *Add/Delete/Change* User. Select option 3, *Change User,* and then click *OK.*

From the drop-down menu, select the store. Now, select the user from the drop-down menu and click Ok.
At this point, you can change the password.

By default, the *System* is the user ID that will function as the Password Administrator for *High-security Passwords.* This user ID does not require any additional setup.
Make sure that you do not activate *High-security Passwords* for the System user ID.

If the user ID is not *System,* then in *the High-Security Passwords* field, select *Y*. In the *Password* field, enter a new password.

The new password should be seven characters long, with one alphabetic and one numeric character. The password cannot be the same as the last four passwords used.

Set a 30-day reminder to change the password for one of the two users. This will keep the passwords from expiring at the same time.

In the *Check Pswd at POS* field, select *Y.* Click *Ok.* Set at least 2 users to high-security passwords.

Setting Up Alerts

Let’s set up alerts to inform users when their passwords are about to expire. From the Home page, Select System Management and then Alerts viewer.

Select *MISC.* Choose *Maintain alert user profiles.*

In the *User field*, select the user with a high-security password from the drop-down menu.

In the *Alert Refresh Frequency field,* enter the amount of time that should elapse between refreshing the current alerts in the system.

Enter the number of days in the *Days in advance to view reminders* field.

Select the *User password expiration warning.* Set the columns *Receive Alerts* and *Receive Email* to *Yes.*

Select **Change** to save. Repeat the same procedure for other users.

Recap

With some initial setup, you can now quickly and efficiently complete payments, making your customers happy.

The contents of this document are for informational purposes only and are subject to change without notice. Epicor Software Corporation makes no guarantee, representations or warranties with regard to the enclosed information and specifically disclaims, to the full extent of the law, any applicable implied warranties, such as fitness for a particular purpose, merchantability, satisfactory quality or reasonable skill and care. This document and its contents, including the viewpoints, dates and functional content expressed herein are believed to be accurate as of its date of publication. The usage of any Epicor software shall be pursuant to the applicable end user license agreement and the performance of any consulting services by Epicor personnel shall be pursuant to applicable standard services terms and conditions. Usage of the solution(s) described in this document with other Epicor software or third party products may require the purchase of licenses for such other products. Epicor, the Epicor logo, and are trademarks of Epicor Software Corporation, registered in the United States and other countries. All other marks are owned by their respective owners. Copyright © 2021 Epicor Software Corporation. All rights reserved.

About Epicor

Epicor Software Corporation drives business growth. We provide flexible, industry-specific software that is designed around the needs of our manufacturing, distribution, retail, and service industry customers. More than 40 years of experience with our customers' unique business processes and operational requirements is built into every solution—in the cloud, hosted, or on premises. With a deep understanding of your industry, Epicor solutions spur growth while managing complexity. The result is powerful solutions that free your resources so you can grow your business. For more information, connect with Epicor or visit www.epicor.com.

Corporate Office
804 Las Cimas Parkway
Austin, TX 78746
USA
Toll Free: +1.888.448.2636
Direct: +1.512.328.2300
Fax: +1.512.278.5590

Latin America and Caribbean
Blvd. Antonio L. Rodriguez #1882 Int. 104
Plaza Central, Col. Santa Maria
Monterrey, Nuevo Leon, CP 64650
Mexico
Phone: +52.81.1551.7100
Fax: +52.81.1551.7117

Europe, Middle East and Africa
No. 1 The Arena
Downshire Way
Bracknell, Berkshire RG12 1PU
United Kingdom
Phone: +44.1344.468468
Fax: +44.1344.468010

Asia
238A Thomson Road #23-06
Novena Square Tower A
Singapore 307684
Singapore
Phone: +65.6333.8121
Fax: +65.6333.8131

Australia and New Zealand
Suite 2 Level 8,
100 Pacific Highway
North Sydney, NSW 2060
Australia
Phone: +61.2.9927.6200
Fax: +61.2.9927.6298